

**U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies
Testimony of Paul Benda
Acting Deputy Under Secretary for Science and Technology Directorate
Department of Homeland Security**

May 26, 2011

The Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002

Good afternoon, Chairman Lungren, Ranking Member Clarke and distinguished Members of the Subcommittee. I am honored to appear before you today on behalf of the Department of Homeland Security (DHS) Science and Technology Directorate (S&T). The Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, enacted by Congress as part of the Homeland Security Act of 2002, has had a prominent role in improving the security of the United States. The SAFETY Act provides incentives for the development and deployment of effective anti-terrorism technologies through systems of risk and litigation management. The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or sellers and users of anti-terrorism technologies from developing and commercializing technologies that could save lives. The Act creates certain liability limitations for claims arising out of, relating to, or resulting from an act of terrorism where “qualified anti-terrorism technologies” have been deployed. My testimony will discuss program performance, the application review process and how S&T is using this important tool to incentivize the development and widespread, high-impact deployment of effective anti-terrorism technologies and services throughout the United States.

Strong Interest, Steadfast Support

The SAFETY Act Program continues to be very popular with the private sector and the Department has continued its steadfast support for the Program. Since the first applications were received in 2004, more than 440 “qualified anti-terrorism technologies” under the SAFETY Act have been approved. These technologies have been widely deployed to protect commercial

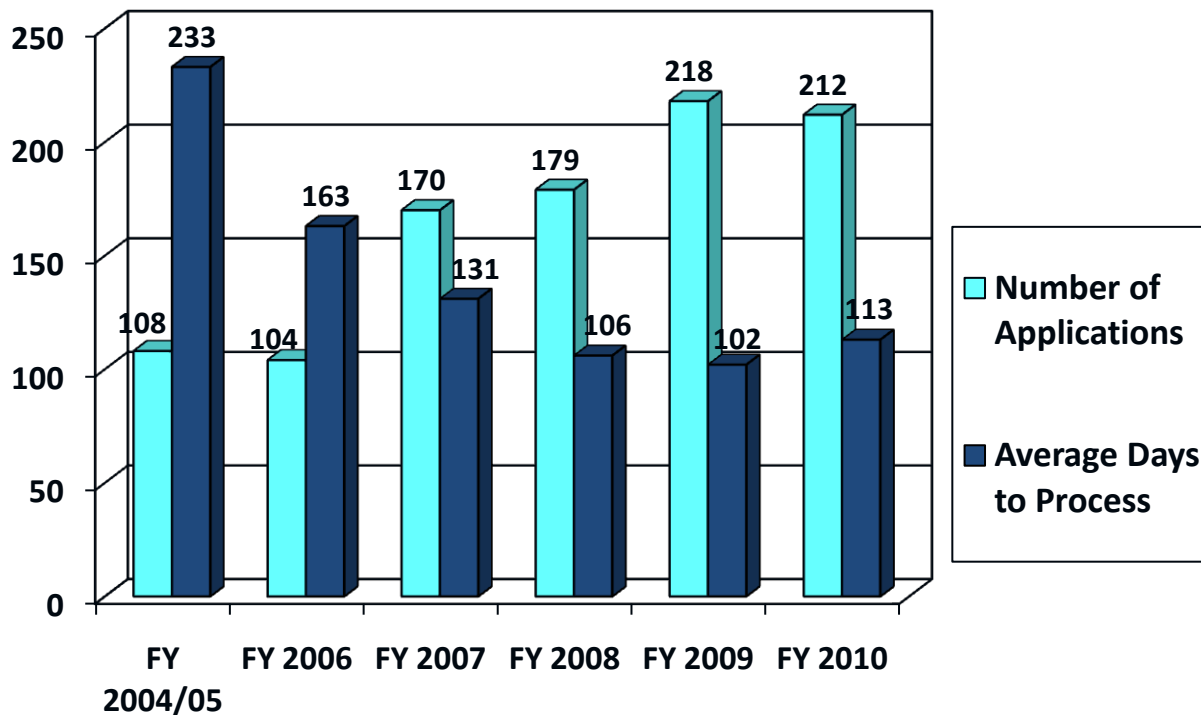
facilities, critical infrastructure, transportation hubs, ports, borders, sports venues and commercial aviation. Examples representing the broad scope of SAFETY Act protections that have been approved during Under Secretary O'Toole's tenure include:

1. A technology that provides cybersecurity situational awareness and network security monitoring.
2. A technology undergoing testing and evaluation designed to provide cybersecurity protection for the smart grid.
3. Technologies designed to harden bridges and tunnels in New York City.
4. An integrated system technology undergoing testing and evaluation designed to provide situational awareness for the Port of Long Beach, California.
5. A modular, rapidly deployable floating security barrier system designed to protect targets from high speed small boats.
6. Anti-terrorism physical security services deployed to detect, deter, and respond to a variety of threats at commercial facilities and adjacent critical infrastructure in the New York Metropolitan area and in New Jersey.
7. A process for the production of an ammonium nitrate fertilizer treated to render it less detonable than standard fertilizer.
8. Onsite production system for chlorine at water treatment plants (eliminating transport risk of bulk chlorine).
9. Threatening object- and explosive-detection systems deployed in the nation's airports.
10. A web-based software tool that integrates a first responder decision support system with geospatial information technology.
11. An acoustic detection system to detect and rapidly triangulate gunshots and explosive event sounds.
12. Explosive containment vessels, allowing for the safe containment, transport and disposal of explosive devices (used in response to Times Square bombing attempt in May 2010).

These SAFETY Act Designations and Certifications have increased the nation's anti-terrorism readiness as well as our domestic industrial capability in the homeland security sector.

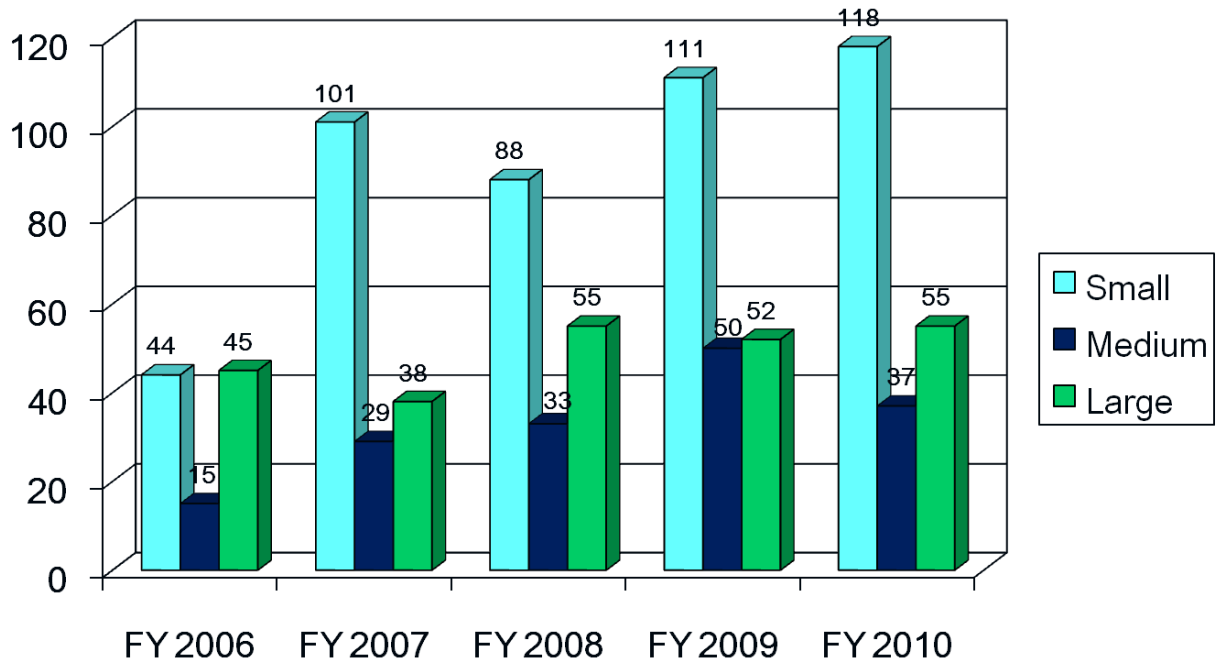
SAFETY Act Progress

Figure 1: SAFETY Act Applications and Processing Time



As shown in Figure 1, applications have doubled since Fiscal Year (FY) 2006, while average application processing times have been reduced by more than 30 percent. This trend has continued into FY 11, where we are expecting 200 to 250 applications with a processing time currently averaging 113 days. As shown below in Figure 2, the majority of program applicants are from smaller businesses. For the purpose of Figure 2, we have grouped businesses with annual revenues under \$50 million as small business. So far in FY 11, small business applicants comprise two-thirds of the applicant pool, with average annual revenues for this group at less than \$11 million.

Figure 2: Applications by Company Size



Small: \$0 - \$50 million; Medium: \$50 million - \$1billion; Large: \$1billion+

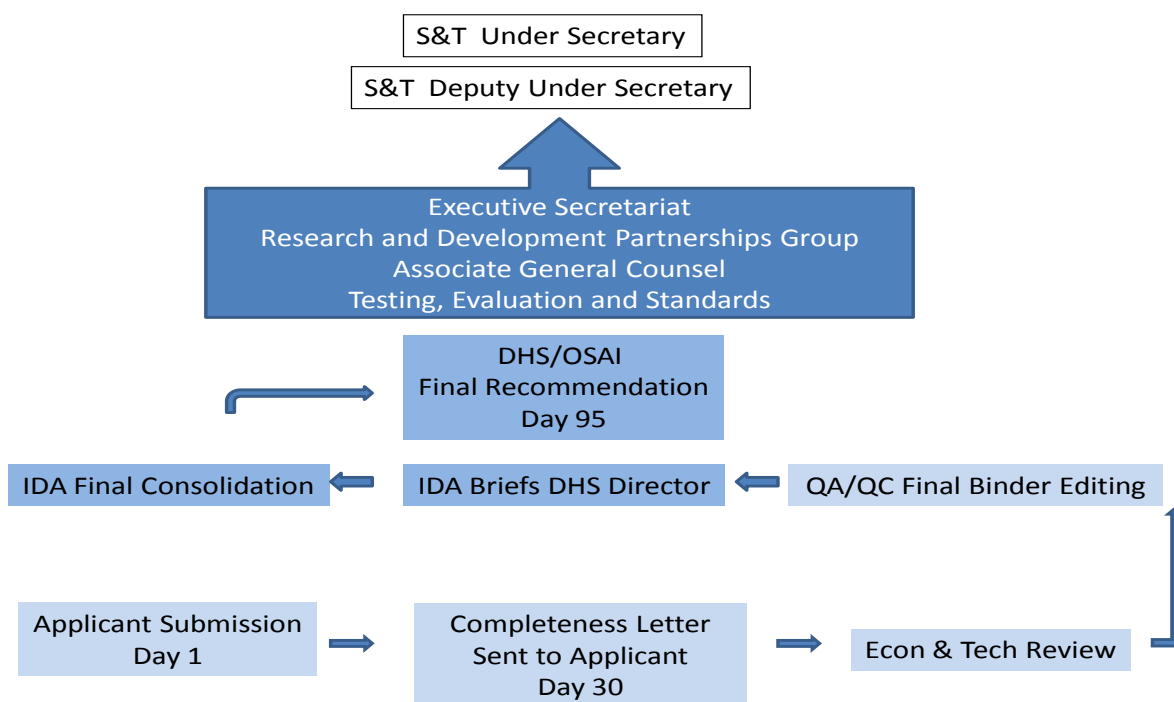
Figure 3 is a flow diagram of the review process used to evaluate SAFETY Act applications. Due to the significance of a SAFETY Act Designation or Certification, considerable thought and effort were devoted to developing a review process that is well-defined, repeatable, and applicable for evaluating both product and service based technologies against the SAFETY Act statutory and regulatory criteria.

Applications are filed electronically via the SAFETY Act website at www.safetyact.gov. Before an applicant submits a full application, they may choose to submit a pre-application, which is an abbreviated application, primarily containing narrative information. This summary process is designed primarily for first time applicants or for those with a unique offering so they can receive prompt feedback and guidance on the scope of information they should submit in order to maximize the chance of success. Within 21 days of application receipt, the Office of SAFETY Act Implementation (OSAI) transmits a letter to the applicant's SAFETY Act account

on the website and offers to hold a teleconference with the applicant to discuss their technology and prospective application for Designation, or Designation and Certification.¹ OSAI technical and economic reviewers participate in the calls; the length and level of detail discussed during the calls is determined by applicant need.

Applications filed for Designation or Designation and Certification are evaluated as follows:

Figure 3: SAFETY Act Application Review Process



Submission – Completeness Phase

During the completeness phase, a submission undergoes a brief review to determine if the information submitted by the applicant is sufficient to conduct a review of a proposed Qualified Anti-Terrorism Technology (QATT) with respect to the statutory and regulatory criteria. The

¹ For a Designation, liability is capped at the amount of liability insurance that DHS requires the technology seller to obtain and maintain. A Certification has a rebuttable presumption that the government contractor defense applies. The presumption may be overcome only by clear and convincing evidence showing that the seller acted fraudulently or with willful misconduct in submitting information to DHS in its SAFETY Act application.

goal of this phase is to determine whether it appears that there is sufficient information in the application to receive an informed evaluation from the expert reviewers who conduct the full technical and economic review. Review personnel who are employees of the Institute for Defense Analyses² (IDA) and who have significant SAFETY Act Program experience perform this completeness review. On or about day 30, if the application appears to have sufficient material to permit a full review, a completeness letter is sent to the applicant. The completeness letter asks the applicant to confirm the technology description drafted by OSAI, and OSAI's summary of the insurance the applicant holds. Completeness letters often have a short list of questions for the applicant, which they should be capable of answering relatively quickly (normally the applicant is given 21 days to provide this information).

If an application appears to not have sufficient material to permit a full review, the applicant receives an incompleteness letter with a listing and discussion of the items that are needed to complete an application. Reasons an application could be determined to be incomplete include: (1) the applicant does not provide enough information to develop a definition of the technology, which is an essential element of any SAFETY Act Designation or Certification; (2) the applicant does not answer significant questions on the application form; (3) the materials submitted support only part of a technology's capabilities (e.g., for an integrated system, information is provided on the video sensor, but no information on the chemical and radiological sensors); (4) the applicant makes a material claim concerning the capability of the technology that is not substantiated by the evidence provided; and/or (5) documents submitted are incomplete or internally inconsistent (training records submitted are inconsistent with stated training policy, test report stating that a significant part of the testing was not conducted, performance report that indicates a significant failure rate).³ Completeness/incompleteness letters are carefully reviewed and signed by the Director of OSAI prior to release to the applicant. An incompleteness letter is posted to the applicant's online application account as soon as the letter is finalized. Normally, this occurs near the 30 day point, but could be much earlier, if there are significant deficiencies in the application that are readily apparent to reviewers.

² IDA, a Federally Funded Research and Development Center, provides technical and expert assistance to the Office of SAFETY Act Implementation. IDA is contracted for these services under an Inter-Agency Agreement.

³ The SAFETY Act Program offers a wide variety of opportunities for applicants to learn what level of information/data they should submit in an application. Opportunities and resources include the pre-application process, teleconference or in person meeting with senior review and program staff, and the SAFETY Act help desk, a resource that is reachable by phone or email.

We believe this approach is preferable to proceeding on with a full review, in spite of identified deficiencies in the application, where the likely end result would likely be a denial letter.

Receiving an incompleteness letter could result in the applicant receiving a favorable decision on its application earlier than if it had to wait to receive a denial letter at or near the 120 day point to learn what is required to prepare a successful application. It also conserves government resources. The S&T Directorate frequently uses independent Subject Matter Experts (SMEs) to conduct the technical and economic reviews following the completeness phase. Having these experts file reports which state that insufficient information was submitted for them to render an opinion concerning the efficacy of the technology is not a prudent use of scarce program resources.

Full Technical and Economic Review

If sufficient information for analysis exists, the application enters the economic and technical review phase. The application and supporting documentation is reviewed by economic and technical SMEs to the OSAI. Concurrently, the IDA staff evaluators conduct independent research on the technology of interest (including discussions with points of contact with federal, state, local and private sector technology users). Following the SMEs review, summary findings, independent research, insurance and economic information are assessed in relation to the statutory and regulatory criteria by internal, independent experts. Following a thorough internal peer review and quality assurance process, a completed analysis is prepared by IDA for review by the Director of OSAI. The Director, based on these independent findings and his/her own knowledge, on or about day 95 following application submission, provides a written report containing a recommendation concerning the appropriate level of SAFETY Act protection and a proposed liability insurance requirement, and selected application materials to the Office of the Under Secretary, Science & Technology, Department of Homeland Security.

Office of the Under Secretary, S&T Review

During this final phase, the application is first reviewed by the S&T Testing and Evaluation Support executive. Areas of review include evidence of technical efficacy, application of relevant standards, a review of any testing and evaluation performed, and, drawing on extensive background and contacts in the testing and evaluation field, whether there are stakeholders or

experts in the interagency who should be consulted. Second, the application moves to the DHS Office of the General Counsel (OGC), which evaluates the sufficiency of the review process (i.e. whether the record adequately reflects adherence to the policies, procedures, and criteria set forth in the SAFETY Act statute and the Department's implementing regulations), the determination of the recommended insurance liability cap, the sufficiency and appropriateness of the description of the covered technology in the Exhibit A Technology Description document, and the content of the proposed SAFETY Act award letters (including the date of first sale of the technology, the correct listing of all named sellers and their states of incorporation and any specific terms and conditions pertaining to the particular award). Third, the application is reviewed by the Director of the Research and Development Partnerships (RDP) Group, who has direct supervisory authority and responsibility over the OSAI. Lastly, the application moves to the S&T Executive Secretariat, where the award documents undergo a brief administrative review, before moving to the Office of the Deputy Under Secretary, who is the Under Secretary's designee for signing SAFETY Act awards. Those applications that present significant policy issues are referred by the Deputy Under Secretary to the Under Secretary for final decision.

Each application's progress is tracked by a spreadsheet, updated weekly, that contains completion of milestones and current status of the review.

SAFETY Act as Incentivizer

The SAFETY Act was designed to incentivize the development and wide-spread deployment of effective anti-terrorism technologies. In implementing this powerful tool, the Department has used a two-prong approach: (1) incentivize private sector entities to build effective anti-terrorism capabilities that they determine to be appropriate using their requirements, analyses and considerable judgment, and (2) increase the accessibility, reach and impact of government homeland security initiatives. Most of the Designations and Certifications to date reflect the judgments of private sector providers and purchasers of anti-terrorism technologies and services delivered through the free market.

Support for government initiatives is provided principally through two processes: (1) a procurement Pre-Qualification Designation Notice, which provides advance notice that private sector entities selected to perform under a listed government procurement will likely qualify for SAFETY Act protections related to their performance, and (2) Block Designations or Block Certifications, which provide notice that private sector entities who provide, whether to private sector or public purchasers, certain technologies or services which meet defined performance standards or technical characteristics are likely to be approved for SAFETY Act protections for those products or services.

As an example, a very popular procurement Pre-Qualification Designation (recently converted to a Block Designation) is for the Transportation Security Administration's (TSA) Certified Cargo Screening Program. This Program involves private sector-owned and -operated secure facilities established in accordance with TSA directives for the screening and securing of cargo to be transported on commercial aircraft. We have issued more than 40 Designations under this Program; many participants are small companies who do not have the revenue to purchase large amounts of terrorism liability insurance. Other procurement Pre-Qualification Designation Notices are listed on the SAFETY Act website. Despite this and other noteworthy successes, the Department has recognized the challenges in applying the SAFETY Act with respect to federal procurements. An effort initiated to better inform the federal acquisition community of the SAFETY Act and how it can be incorporated effectively is nearing completion. The Federal Acquisition Institute (FAI), in collaboration with the Department, is developing a multimedia, online training course that will help acquisition personnel properly apply the SAFETY Act to an acquisition. FAI and DHS anticipate launching the SAFETY Act and Federal Acquisition course by summer.

We are also seeking to use Block Designations and Block Certifications more often as they are powerful tools to incentivize deployment of anti-terrorism technologies and offer an expedited review timeline. S&T recognizes that the SAFETY Act application process requires a significant investment by the applicant who would like us to process their applications more quickly. While we consistently meet the application processing timelines set forth in the SAFETY Act Final Rule, we are looking at expanding our use of Block Designations, which are processed 25

percent faster than standard applications. Our goal is to streamline our Block review process and speed processing timelines to be 30 to 50 percent faster than standard applications and provide an expedited review path for appropriate technologies.

An example of a recently approved Block Designation and Block Certification is for standards development organizations who wish to seek SAFETY Act coverage for national standards that have been formally adopted by DHS as DHS National Standards. Recently, as a result of an S&T policy review, the opportunity to receive SAFETY Act coverage for a broader range of anti-terrorism standards has been approved and announced on the SAFETY Act website. The intent of this initiative is to provide incentives for increased use and more widespread implementation of anti-terrorism standards, by significantly expanding the pool of standards eligible for SAFETY Act coverage. This initiative has strong industry interest.

S&T has also partnered with the DHS Domestic Nuclear Detection Office (DNDO) to create a new Block Designation to incentivize the deployment of nuclear detection technologies. The DNDO Graduated Radiological/Nuclear Detector Evaluation and Reporting (GRaDER) Program, which evaluates commercial off the shelf Radiological/Nuclear detection equipment against national standards, has developed a mechanism for manufacturers to independently verify the performance of their technologies. The Block Designation will apply to technologies having undergone testing in accordance with the GRaDER program that have fully met the American National Standard Institute N42 standard or applicable published Government standards.

The SAFETY Act is also involved as an integral part of other DHS programs and projects. In S&T, the SAFETY Act will help incentivize private sector involvement in our newest APEX projects, which are projects that have been endorsed by both a DHS component head and the Under Secretary of Science and Technology through a signed charter. The goals of the APEX projects are to transition high-impact technology-based capabilities directly into components operational programs. Our most recently signed APEX project with the U.S. Customs and Border Protection (CBP) is to leverage Customs-Trade Partnership Against Terrorism (C-TPAT) Tier III shipper's approved security plans and operations with an Electronic Chain of Custody (ECoC) lock that S&T developed to create a "Secure Transit Corridor" with supply chain routes

originating from Mexico and Canada to allow expedited security screening at CBP selected pilot ports of entry. If this pilot is successful, we hope to incentivize adoption of this model by private industry by creating a Block Designation for commercial shippers who agree to deploy the ECoCs and follow the stringent security standards required of C-TPAT Tier III shippers. This effort will improve overall supply chain security while at the same time expedite the free flow of trade and reduce liability insurance costs of participating shippers.

We are also actively engaged in several other initiatives – concerning cybersecurity, infrastructure protection, stadium security, transportation security and private sector resilience – that will use the SAFETY Act to strengthen and enhance the security of the nation. As you can see, this is a dynamic program that is continually evolving to meet the needs of the government in true partnership with the private and public sectors.

Conclusion

In closing, I would like to thank you for the invitation to appear before you today and your continuing support of the SAFETY Act. I look forward to answering your questions and to working with you on maintaining the vitality of this very important program.